APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/768,518	01/30/2004	Ali Murat Iloglu	Iloglu 2003-0125	6635

7590 04/10/2007	EXAMINER
Henry T. Brendzel P.O. Box 574 Springfield, NJ 07081	BELANI, KISHIN G

ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

PTOL-90A (Rev. 10/06)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>01/30/2004</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-21</u> is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-17 and 21</u> is/are rejected.

7)☐ Claim(s) <u>18-20</u> is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>30 January 2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date <u>7/14/2005</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____ .

DETAILED ACTION

Priority

Applicant's claim for domestic priority under 35 U.S.C. 119 (e) is acknowledged.

Information Disclosure Statement

The information disclosure statement submitted on 07-14-2005 has been

considered by the Examiner and made of record in the application file.

Preliminary Amendment

The present Office Action is based upon the original patent application filed on

01/30/2004 as modified by the preliminary amendment filed on 01/16/2007. Claims 1-

21 are now pending in the present application.

Specification

The disclosure is objected to because of the following informalities:

In paragraph 007, line 8; replace "in the case he" by – in the case the –

In paragraph 016 (paragraph just below TABLE I), line 8; replace "CRF" by – VRF –

In paragraph 017, line 1; replace "100 within network 100" by – 110 within network 100

–.

Appropriate correction is required.

Claim Objections

Claims 1, 4, 7, and 14 are objected to because of the following informalities:

In **claim 1**, the examiner has interpreted the phrase "assigned VPN cannot establish" as

– assigned VPN, and therefore cannot establish –.

In **claim 4**, change "clam 1" to – claim 1 –

In **claim 7**, change two occurrences of "though" to – through –.

In **claim 14**, change "from system B from" to – from system B to –.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining

obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness
   or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-6, 8, 10, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Chantrain et al. (U.S. Patent Application Publication # 2002/0002687 A1)** in view of **Chu et al. (U.S. Patent Application Publication # 2004/0255028 A1)**.

Consider **claim 1**, Chantrain et al. clearly show and disclose an arrangement comprising a network adapted to allow systems to connect to the network, and further adapted to assign at least some of said systems to specified VPNs (Fig. 1 in which a user 111 communicates with server 163 belonging to VPN 152 (corresponding to system A of claim 1 specified below) as well as communicates with server 161 using local VPN 151 (corresponding to system B of claim 1 specified below); and a user 112 communicates with server 164 belonging to VPN 153, both using the core network 14; paragraphs 0025 and 0031 that describe various elements of the arrangement mentioned in the claim),

which network includes collection of modules that includes one or more devices that

operate to not enable systems A and B of said systems that are each assigned to one

or more VPNs but which have no commonly assigned VPN, and therefore cannot

establish connection to each other (paragraph 0002, lines 3-8 which disclose severe

access restrictions placed on the third party or corporate VPNs by not allowing access

through these VPNs), characterized by:

a controller (110-200) that

(1) detects an identified application, executed in an element of said arrangement, which

calls for communication between system A and system B (paragraph 0030 that

discloses a controller NAS 131 (shown in Fig. 1) storing source and destination IP

addresses as well as VPN IDs in a table during a voice or a data connection setup as

disclosed in paragraph 0023; paragraph 0031 that discloses how the NAS 131 controller

detects the VPN 151's route from a message destined to server 161 from the user 111

who is already connected to VPN 152), and

(2) authorizes such communication when said identified application is included in a set

of one or more allowed applications, by directing said collection of elements to modify

itself to enable said establishing a connection between system A and system B

(paragraph 0020 that discloses how NASs 131, 132 enable the access of end-users

111-114 to the core network 14 and to the interconnected data communication networks

151-153 by using authentication servers 161-164; paragraph 0033 that discloses how

NAS 131 directs a message destined to a server 161 not belonging to the VPN 152 to

which user 111 is already connected, by directing it on a logical channel assigned the identifier of VPN 152).

However, Chantrain et al. do not specifically disclose that the systems connect to the network via edge routers of the network.

In the same field of endeavor, Chu et al. clearly show and disclose that the systems connect to the network via edge routers of the network (Fig. 1 that shows four edge routers marked PE 108_1, 108_2, 108_3, and 108_m, forming an edge network 104 and connecting the service provider's network 102 to the customer's networks 120_1, 120_2, 120_3, and 120_p via customer's edge routers 122_1, 122_2, 122_3, and 122_p; paragraph 0029 that discloses how the customer networks are connected to the service provider's network by edge routers 108 (PE)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to connect customer networks to the service provider's network via edge routers of the network, as taught by Chu et al. in the arrangement of Chantrain et al, so as to provide customer networks access to voice and data services via service provider's network and the Internet by secure means offered by Virtual Private Network (VPN).

Consider **claim 2,** and **as applied to claim 1 above**, Chantrain et al. as modified by Chu et al., further disclose an arrangement where said element of said arrangement is system A (Fig. 1 in which a user 111 communicates with server 163 belonging to VPN 152, thereby disclosing system A of the claim).

Consider **claim 3,** and **as applied to claim 1 above**, Chantrain et al. as modified by Chu et al., further disclose an arrangement where said element of said arrangement is system B (user 111 communicates with server 161 using local VPN 151, thereby disclosing system B of the claim).

Consider **claim 4,** and **as applied to claim 1 above**, Chantrain et al. as modified by Chu et al., disclose the claimed invention except disclosing an arrangement where said collection of modules comprises said edge routers.

In the same field of endeavor, Chu et al. clearly show and disclose an arrangement where said collection of modules comprises said edge routers (Fig. 1 that shows four edge routers marked PE 108_1, 108_2, 108_3, and 108_m, forming an edge network 104 and connecting the service provider's network 102 to the customer's networks 120_1, 120_2, 120_3, and 120_p via customer's edge routers 122_1, 122_2, 122_3, and 122_p; paragraph 0029 that discloses how the customer networks are connected to the service provider's network by edge routers 108 (PE)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to connect customer networks to the service provider's network via edge routers of the network, as taught by Chu et al. in the arrangement of Chantrain et al, so as to provide customer networks access to voice and data services via service provider's network and the Internet by secure means offered by Virtual Private Network (VPN).

Consider **claim 5,** and **as applied to claim 1 above**, Chantrain et al. as modified by Chu et al., disclose the claimed invention except an arrangement where said collection of modules comprises VPN routing and forwarding tables, one within each of said edge routers.

In the same field of endeavor, Chu et al. clearly disclose an arrangement where said collection of modules comprises VPN routing and forwarding tables, one within each of said edge routers (paragraph 0004, lines 1-4 that disclose the presence of routing tables within each PE router, populated in a VPN Routing Forwarding (VRF) table).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide a collection of modules comprising VPN routing and forwarding tables, one within each of said edge routers, as taught by Chu et al. in the arrangement of Chantrain et al. as modified by Chu et al., so that the messages originating at a customer site can be forwarded to the specified location via an associated VPN path, by referencing the VRF tables.

Consider **claim 6,** and **as applied to claim 1 above**, Chantrain et al. as modified by Chu et al., disclose the claimed invention except an arrangement where said network is an MPLS network.

In the same field of endeavor, Chu et al. clearly disclose an arrangement where said network is an MPLS network (paragraph 0028, lines 5-8 which disclose that MPLS is used for forwarding packets of data over the network).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide an MPLS network for forwarding packets of data over the network, as taught by Chu et al. in the arrangement of Chantrain et al. as modified by Chu et al., as MPLS is more popular of the two protocols commonly used for service provider based IP-VPN protocols.

Consider **claim 8,** and **as applied to claim 1 above,** Chantrain et al. as modified by Chu et al., further disclose an arrangement where said identified application is voice over IP and voice over IP is one of said allowed applications (Fig. 1, core network block 14; paragraph 0019 which discloses that the core network may be the public Internet; paragraph 0023 which teaches that access networks 121 and 122 may be PSTN (voice calls) networks; thereby disclosing provision for the VoIP applications).

Consider **claim 10,** and **as applied to claim 1 above,** Chantrain et al. as modified by Chu et al., further disclose an arrangement where said controller comprises a route server and a call control element (paragraph 0024 which discloses that for telephone networks, NASs 131, 132 comprise analog modems and a router function and a gateway to the core network; paragraph 0030, lines 1-4 which disclose call control function of NAS 131).

Consider **claim 21**, Chantrain et al. clearly show and disclose a method executed

in an arrangement including a network that supports assigning systems to specified

VPNs (Fig. 1 in which a user 111 communicates with server 163 belonging to VPN 152

(corresponding to system A of claim 21 specified below) as well as communicates with

server 161 using local VPN 151 (corresponding to system B of claim 21 specified

below); and a user 112 communicates with server 164 belonging to VPN 153, both

using the core network 14; paragraphs 0025 and 0031 that describe various elements of

the arrangement mentioned in the claim),

which network includes collection of modules, comprising one or more devices, that

operates to insure that systems A and B of said systems that are each assigned to one

or more VPNs but which have no commonly assigned VPN are disallowed to

communicate with each othe (paragraph 0002, lines 3-8 which disclose severe access

restrictions placed on the third party or corporate VPNs by not allowing access through

these VPNs), characterized by the steps of:

receiving a message indicating a desire to establish communication between said

systems A and B pursuant to an identified application (paragraph 0030 that discloses a

controller NAS 131 (shown in Fig. 1) storing source and destination IP addresses as

well as VPN IDs in a table during a voice or a data connection setup as disclosed in

paragraph 0023; paragraph 0031 that discloses how the NAS 131 controller detects the

VPN 151's route from a message destined to server 161 from the user 111 who is

already connected to VPN 152);

determining whether to authorize said communication (paragraph 0020 that discloses

how NASs 131, 132 enable the access of end-users 111-114 to the core network 14

and to the interconnected data communication networks 151-153 by using

authentication servers 161-164); and

when said step of determining concludes that such communication ought to be

permitted, directing said collection of modules to allow said communication (paragraph

0033 that discloses how NAS 131 directs a message destined to a server 161 not

belonging to the VPN 152 to which user 111 is already connected, by directing it on a

logical channel assigned the identifier of VPN 152).

     However, Chantrain et al. do not specifically disclose that the systems connect to

edge routers of the network.

     In the same field of endeavor, Chu et al. clearly show and disclose that the

systems connect to the network via edge routers of the network (Fig. 1 that shows four

edge routers marked PE 108_1, 108_2, 108_3, and 108_m, forming an edge network 104 and

connecting the service provider's network 102 to the customer's networks 120_1, 120_2,

120_3, and 120_p via customer's edge routers 122_1, 122_2, 122_3, and 122_p; paragraph 0029

that discloses how the customer networks are connected to the service provider's

network by edge routers 108 (PE)).

     Therefore, it would have been obvious to a person of ordinary skill in the art at

the time the invention was made to connect customer networks to the service provider's

network via edge routers of the network, as taught by Chu et al. in the method of

Chantrain et al, so as to provide customers' networks access to voice and data services

via service provider's network and the Internet, by secure means offered by Virtual

Private Network (VPN).

Claims 7, 9, 11-17 are rejected under 35 U.S.C. 103(a) as being unpatentable

over **Chantrain et al. (U.S. Patent Application Publication # 2002/0002687 A1)** in

view of **Chu et al. (U.S. Patent Application Publication # 2004/0255028 A1)**, and

further in view of **Salama (U.S. Patent Publication # 7,120,682 B1)**.

Consider **claim 7**, and **as applied to claim 1 above**, Chantrain et al. as modified

by Chu et al., disclose the claimed invention except disclosing that said collection of

modules comprises VPN routing and forwarding tables, one within each of edge routers

of said network, and said controller directs an edge router of said edge routers through

which system A is connected to said network to modify its routing and forwarding table,

and directs an edge router of said edge routers through which system B is connected to

said network to modify its routing and forwarding table.

In the same field of endeavor, Salama discloses that said collection of modules

comprises VPN routing and forwarding tables, one within each of edge routers of said

network, and said controller directs an edge router of said edge routers through which

system A is connected to said network to modify its routing and forwarding table, and

directs an edge router of said edge routers through which system B is connected to said

network to modify its routing and forwarding table (Fig. 2; column 4, lines 4-23 which

disclose a method to call outside the VPN by using global routing information database

and leaking (interpreted by the examiner to mean temporarily copying) information from the global routing information database into the routing information database of that customer).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide a collection of modules comprising VPN routing and forwarding tables, one within each of edge routers of said network, and said controller directing an edge router of said edge routers through which system A is connected to said network to modify its routing and forwarding table, and directs an edge router of said edge routers through which system B is connected to said network to modify its routing and forwarding table, as taught by Salama in the arrangement of Chantrain et al. as modified by Chu et al., so as to provide means for a user connected to a VPN via the Internet to securely communicate with others not belonging to the same VPN.

Consider **claim 9,** and **as applied to claim 1 above**, Chantrain et al. as modified by Chu et al., disclose the claimed invention except disclosing that said identified application is video over IP and video over IP is one of said allowed applications.

In the same field of endeavor, Salama discloses that said identified application is video over IP and video over IP is one of said allowed applications (column 1, lines 12-14 and lines 27-34 which disclose that video over IP is being offered over service providers' data networks via VPNs).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide video over IP service, as taught by Salama in the arrangement of Chantrain et al. as modified by Chu et al., so as to utilize the spare capacity of the service providers' networks combined with the secure VPN to offer desired services to their customers.

Consider **claim 11**, and **as applied to claim 21 above**, Chantrain et al. as modified by Chu et al., further disclose the claimed invention including directing said collection of modules to remove said modification at a later time to reinstate prohibition against communication between said systems A and B (paragraph 0027 which discloses that the IP address for connection set up and the VPN ID to be connected to, are assigned to the user only for the connection duration of the call, thereby disclosing that the modifications are deleted at the end of the call to reinstate prohibition against communication between said systems A and B).

However, Chantrain et al. as modified by Chu et al., do not specifically disclose a method where the step of directing said collection of modules to allow said communication comprises directing said collection of modules to install a modification whose effect is to allow communication between said systems A and B.

In the same field of endeavor, Salama discloses a method where the step of directing said collection of modules to allow said communication comprises: directing said collection of modules to install a modification whose effect is to allow communication between said systems A and B (Fig. 2; column 4, lines 4-23 which

disclose a method to call outside the VPN by using global routing information database
and leaking (interpreted by the examiner to mean temporarily copying) information from
the global routing information database into the routing information database of that
customer).

Therefore, it would have been obvious to a person of ordinary skill in the art at
the time the invention was made to provide a method where the step of directing said
collection of modules to allow said communication comprises directing said collection of
modules to install a modification whose effect is to allow communication between said
systems A and B, as taught by Salama in the arrangement of Chantrain et al. as
modified by Chu et al., so as to provide means for a user connected to a VPN via the
Internet to securely communicate with others not belonging to the same VPN.

Consider **claim 12**, and **as applied to claim 11 above**, Chantrain et al. as
modified by Chu et al., and further modified by Salama, further disclose a method where
said application is voice over Internet or video over Internet (Fig. 1, core network block
14; paragraph 0019 which discloses that the core network may be the public Internet;
paragraph 0023 which teaches that access networks 121 and 122 may be PSTN (voice
calls) networks; thereby disclosing provision for the voice over Internet service).

Consider **claim 13**, and **as applied to claim 12 above**, Chantrain et al. as
modified by Chu et al., and further modified by Salama, further disclose a method for
the claimed invention where said directing of said collection of modules to remove said

modification occurs substantially contemporaneously with termination of said voice over Internet or video over Internet communication (paragraph 0027 which discloses that the IP address for connection set up and the VPN ID to be connected to, are assigned to the user only for the connection duration of the call).

Consider **claim 14**, and **as applied to claim 11 above**, Chantrain et al. as modified by Chu et al., disclose the claimed invention except disclosing a method where said directing said collection of modules to install a modification comprises the steps of installing a first entry in a table of an element that of said collection of modules that is charged with blocking traffic so that that no traffic is carried from system A to a system that is assigned to a VPN to which system A is not assigned, which entry nullifies said blocking relative to system B, and installing a second entry in a table of an element of said collection of modules that is charged with blocking traffic so that that no traffic is carried from system B to a system that is assigned to a VPN to which system B is not assigned, which entry nullifies said blocking relative to system A.

In the same field of endeavor, Salama discloses a method where said directing said collection of modules to install a modification comprises the steps of installing a first entry in a table of an element that of said collection of modules that is charged with blocking traffic so that that no traffic is carried from system A to a system that is assigned to a VPN to which system A is not assigned, which entry nullifies said blocking relative to system B, and installing a second entry in a table of an element of said collection of modules that is charged with blocking traffic so that that no traffic is carried

from system B to a system that is assigned to a VPN to which system B is not assigned, which entry nullifies said blocking relative to system A (Fig. 1, server blocks 12 and 14; Fig. 2, Routing Info Table block 20 and VPN Association Table block 22; column 4, lines 4-23 which disclose a method to call outside the VPN by using global routing information database and leaking (interpreted by the examiner to mean temporarily copying) information from the global routing information database into the routing information database of that customer).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide a method where said directing said collection of modules to install a modification comprises the steps of installing a first entry in a table of an element that of said collection of modules that is charged with blocking traffic so that that no traffic is carried from system A to a system that is assigned to a VPN to which system A is not assigned, which entry nullifies said blocking relative to system B, and installing a second entry in a table of an element of said collection of modules that is charged with blocking traffic so that that no traffic is carried from system B to a system that is assigned to a VPN to which system B is not assigned, which entry nullifies said blocking relative to system A, as taught by Salama in the method of Chantrain et al. as modified by Chu et al., so as to provide means for a user connected to a VPN via the Internet to securely communicate with others not belonging to the same VPN.

Consider **claim 15**, and **as applied to claim 14 above**, Chantrain et al. as modified by Chu et al., and further modified by Salama, further disclose a method where the first entry includes a criterion that nullifies said blocking only relative to traffic pertaining to said application, and the second entry includes a criterion that nullifies said blocking only relative to traffic pertaining to said application (paragraph 0027 which discloses that the IP address for connection set up and the VPN ID to be connected to, are assigned to the user only for the duration of the VoIP call set up).

Consider **claim 16**, and **as applied to claim 11 above**, Chantrain et al. as modified by Chu et al., and further modified by Salama, further disclose a method where said collection of modules is said edge routers of the network (Fig. 1 (Chu et al.) that shows four edge routers marked PE 108_1, 108_2, 108_3, and 108_m, forming an edge network 104 and connecting the service provider's network 102 to the customer's networks 120_1, 120_2, 120_3, and 120_p via customer's edge routers 122_1, 122_2, 122_3, and 122_p; paragraph 0029 that discloses how the customer networks are connected to the service provider's network by edge routers 108 (PE)).

Consider **claim 17**, and **as applied to claim 11 above**, Chantrain et al. as modified by Chu et al., and further modified by Salama, further disclose a method where said directing said collection of modules to install a modification comprises a step of installing a entry in a VPN route and forward (VRF) table that is associated with edge router A of said edge routes through which said system A is coupled to said network,

and installing an entry in a VRF table that is associated with edge router B of said edge

routes through which said system B is coupled to said network (Fig. 2 (Salama) that

shows Routing Info Table 20 and Association Table 22, linked by VPN ID, such that

whenever a data packet for a VPN ID is received at port 24 from the Gateway, the

Routing Info Table is updated if the VPN ID of the packet is not already in the table (as

in the case of VPN B packet); column 4, lines 11-15, which disclose the updating of the

Routing Info Table 20).

Allowable Subject Matter

Claims 18-20 are objected to as being dependent upon a rejected base claim,

but would be allowable if rewritten in independent form including all of the limitations of

the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject

matter:

Consider **claim 18,** the best prior art found during the examination of the present

application, **Chantrain et al. (U.S. Patent Application Publication # 2002/0002687**

A1) in view of **Chu et al. (U.S. Patent Application Publication # 2004/0255028 A1),**

and further in view of **Salama (U.S. Patent Publication # 7,120,682 B1),** fail to

specifically disclose the limitation of the method of arrangement of VPNs in a network,

where said entry that is installed in said VRF associated with said edge router A

comprises an indication that system B belongs to a VPN to which system A belongs,

and said entry that is installed in said VRF associated with said edge router B

comprises an indication that system A belongs to a VPN to which system B belongs.

Claims 19 and 20 are also objected to as being allowable by virtue of their

dependency on **claim 18**.

Conclusion

The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure:

US Patent Application Publication: 2003/0079043 A1, inventor: Chang et al.

Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Art Unit: 2109

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the

Examiner should be directed to Kishin G. Belani whose telephone number is (571) 270-1768. The Examiner can normally be reached on Monday-Thursday from 6:30 am to 5:00 pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Rafael Perez Gutierrez can be reached on (571) 270-1767 or (571) 272-7915. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 703-305-3028.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

Kishin G. Belani
K.G.B./kgb

March 30, 2007

RAFAEL PEREZ-GUTIERREZ
SUPERVISORY PATENT EXAMINER
4/4/07